IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CHRISTAH ROSS, on behalf of her minor daughter; and CARTER BUNDY, on behalf of his minor son, individually and on behalf of all others similarly situated, Plaintiffs, v. NEXTGEN HEALTHCARE INC., Defendant.	Case No.: **JURY TRIAL DEMANDED** **COMPLAINT - CLASS ACTION**

CLASS ACTION COMPLAINT

Plaintiffs Christah Ross, on behalf of her minor daughter, and Carter Bundy, on behalf of his minor son (collectively "Plaintiffs"), individually and on behalf of all persons similarly situated (the "Class" or "Class Members"), by and through the undersigned counsel, bring this class action complaint against Defendant NextGen Healthcare Inc. ("NextGen" or "Defendant"). Plaintiffs make the following allegations based upon personal knowledge with respect to themselves, and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE CASE

1. Plaintiffs bring this class action Complaint against NextGen for its failure to adequately and properly secure and safeguard patients' personally identifiable information ("PII"), and for failing to provide timely, accurate, and adequate notice to Plaintiffs and Class Members that their PII had been compromised.

2. NextGen is a healthcare software company that does business with physicians and healthcare professionals to provide them with health records software and practice management systems.[1] Medical professionals entrust NextGen with sensitive PII from their patients in order to effectively use NextGen's systems. Plaintiffs and Class Members are third-party beneficiaries to the promises made by NextGen to medical professionals.

3. On April 28, 2023, NextGen began notifying state attorney generals and patients that NextGen had experienced a massive data breach in which a cybercriminal obtained unauthorized access to the NextGen systems between at least March 29, 2023, and April 14, 2023 (the "Data Breach").

4. In a data breach notification filed with the Maine Attorney General's Office, NextGen admitted that hackers gained "unauthorized access to database

[1] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last accessed May 16, 2023).

stemming from use of stolen client credentials that appear to have been stolen from other sources or incidents unrelated to NextGen."[2]

5. The same notification filed in Maine, NextGen admitted the total number of affected persons by the Data Breach to be 1,049,375. Although the Maine filing states the breach was discovered on April 24, 2023, the notice NextGen sent out states that NextGen was "alerted to suspicious activity" on the NextGen system on March 30, 2023.

6. According to the NextGen notice sent to consumers, the Data Breach began March 29, 2023. NextGen was, however, unable to stop the breach until April 14, 2023, at the earliest. NextGen's notice letter is not clear that the breach was actually stopped on April 14, 2023.

7. Although NextGen learned of the breach on March 30, 2023, it failed to inform affected consumers and the Class Members until almost a month later on April 28, 2023.

8. The Data Breach occurred and was amplified by NextGen's negligent failure to implement reasonable and adequate security procedures and practices, its failure to disclose material facts surrounding its deficient data security protocols, and its failure to timely notify the victims of the Data Breach.

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/cb1d4654-0ce0-4e59-9eec-24391249e2a8.shtml (last accessed May 16, 2023).

9. As a result of NextGen's failure to protect the sensitive PII it was entrusted to safeguard, Plaintiffs and Class members have already suffered harm and have been exposed to a significant and continuing risk of identity theft, financial fraud, and other identity-related fraud for years to come.

PARTIES

10. Plaintiff Christah Ross and her minor daughter are residents and citizens of Dickson, Tennessee. During May 2023, Ms. Ross was notified via letter from NexGen that her daughter, K.R., was a victim of the Data Breach.

11. Plaintiff Carter Bundy and his minor son are residents and citizens of Santa Fe, New Mexico. During May 2023, Mr. Bundy was notified via letter from NextGen that his son, A.B., was a victim of the Data Breach.

12. Defendant NextGen Healthcare Inc. is a Delaware corporation registered with the state of Georgia as a Foreign Profit Corporation with its principal place of business in Atlanta, Georgia.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant NextGen, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interests and costs. This

Court also has supplemental jurisdiction over the claims in this case pursuant to 28 U.S.C. 1367(a) because all claims alleged herein form part of the same case or controversy under Article III of the United States Constitution.

14. This Court has general personal jurisdiction over Defendant NextGen because NextGen maintains its principal place of business in Atlanta, Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia, such to not offend notions of fair play and substantial justice.

15. Venue in the Northern District of Georgia is proper under 28 U.S.C. § 1391 because NextGen resides in this District, and a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and the Class Members.

FACTUAL ALLEGATIONS

NextGen's Privacy Practices

16. NextGen is an integrated healthcare solutions company that "provides electronic health records and practice management solutions to doctors and medical professionals."[3] NextGen touts is system as "a leading provider of innovative, cloud-

[3] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 16, 2023).

based, healthcare technology solutions that empower healthcare practices to manage the risk and complexity of delivering care in the United States healthcare system."[4]

17. NextGen's website acknowledges the significance of data security. Under the page titled "Elevate your practice's health IT with NextGen Managed Cloud Services" is a warning symbol followed by "Reduce Risk" and "We go to extraordinary lengths to make your data as secure as possible—(1) third-party certification with the Health Information Trust Alliance (HITRUST), (2) collaboration with Amazon Web Services, a platform built to meet requirements of the most security-sensitive organizations."[5]

Reduce risk

We go to extraordinary lengths to make your data as secure as possible—(1) third-party certification with the Health Information Trust Alliance (HITRUST), (2) collaboration with Amazon Web Services, a platform built to meet requirements of the most security-sensitive organizations.

[4] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last accessed May 16, 2023).
[5] https://www.nextgen.com/services/managed-cloud (last accessed May 16, 2023).

18. NextGen also recognized the importance of data security in its SEC filings: "If our security measures are breached or fail and unauthorized access is obtained to a client's data, our services may be perceived as not being secure, clients may curtail or stop using our services, and we may incur significant liabilities."[6]

19. In using NextGen's systems, healthcare professionals provide patients' highly sensitive PII to NextGen through its platforms, including Social Security numbers. Through no choice of patients' own, their highly sensitive PII is then stored on NextGen's inadequately secured and Internet-accessible network.

20. In NextGen's 2022 Form 10-K, it acknowledged the sensitivity and importance of the patients' PII and NextGen's obligation to adequately safeguard it, as well as the risks associated with any failure to do so. "Our services involve the storage, transmission and processing of clients' proprietary information and protected health information of patients. Because of the sensitivity of this information, security features of our software are very important."[7]

21. Because NextGen obtained, collected, and stored Plaintiffs' and Class Members' PII, it assumed legal and equitable responsibilities and knew or should

[6] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last accessed May 16, 2023).
[7] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last accessed May 16, 2023).

have known it was responsible for safeguarding the PII from unauthorized disclosure to criminal third parties.

22. NextGen maintains a privacy policy linked from its website that was updated as of May 9, 2023. Under Section 8 of the Privacy Policy, "Patient Information," states:

> Certain web-based services provided by us . . . involve access to, and the processing of, patient information. This information is provided to us lawfully by: (i) medical professionals who have obtained their patients' consent to provide us with their patient information or (ii) by the patient themselves (or, if the patient is a minor, through their parent or guardian).
>
> Such information may be considered Protected Health Information ("PHI") as that term is defined in the Health Insurance Portability and Accountability Act of 1996, as amended, and its implementing regulations ("HIPAA"). Such information may also be regulated by certain state laws. We process PHI on behalf of our healthcare provider customers and subject to contractual agreements with such customers, including business associate agreements. This Privacy Policy does not apply to our use and disclosure of PHI. If you have any questions or concerns regarding PHI you believe may be processed by our products and services, please contact the health care provider customer with whom you have a relationship directly.[8]

The Data Breach

23. Between at least March 29, 2022, and April 14, 2023, an unauthorized cybercriminal accessed the NextGen network and infiltrated a massive amount of

[8] https://www.nextgen.com/privacy-policy (last accessed May 16, 2023

highly sensitive PII store on the NextGen servers, including full names and Social Security numbers of over one million patients.

24. NextGen was alerted to the existence of the Data Breach on March 30, 2023, but failed to disclose the Data Breach until almost a month later, once it began notifying state attorneys general and affected borrowers on April 28, 2023.

25. In NextGen's notice to state attorneys general, it stated:

a. The breach occurred on March 29, 2023;

b. It discovered the breach on March 30, 2023;

c. NextGen described the breach as "an unknown third-party gained unauthorized access to a limited set of electronically stored personal information"; and

d. The hackers acquired the names or other PII and Social Security numbers of over one million patients.[9]

26. The sample form of NextGen's notice letter to consumers provides the following description:

> On March 30, 2023, we were alerted to suspicious activity on our NextGen Office system. In response, we launched an investigation with the help of third-party forensic experts. We also took measures to contain the incident, including resetting passwords, and contacted law enforcement. Based on our in-depth investigation to date, supported by our external experts, it appears that an unknown third-party gained unauthorized access to a limited set of electronically

[9] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 16, 2023).

> stored personal information between March 29, 2023 and April 14, 2023. As a result of our detailed analysis of the information impacted, we recently determined that certain of your personal information was included in the electronic data accessed during the incident. Below we have provided information about what information was involved, what we are doing in response, and what you can do to proactively protect yourself.[10]

27. Based on NextGen's notification letter, it is not clear exactly when the sensitive PII was taken by the unauthorized third party; when NextGen launched its investigation into the Data Breach; the full extent of what data was accessed; when NextGen took action to stop or mitigate the breach; or whether the Data Breach has actually been stopped as of the date this Complaint is filed.

28. The only actual notice the letter serves to provide is that all or nearly all of the sensitive PII provided by patients was inadequately safeguarded and therefore accessed without authorization.

29. The notice letter also claims that NextGen took action in response to the Data Breach, "[w]e also took measures to contain the incident, including resetting passwords, and contacted law enforcement."[11]

[10] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 16, 2023).
[11] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 16, 2023).

30. What is not discussed in the notice are any details regarding how the PII was accessed by the hackers, or how NextGen's actions may have remediated the root cause of the Data Breach.

31. As of the date this Complaint is filed, NextGen has not posted any alert regarding the Data Breach on its website[12], including on its Press Release page[13], or page titled "In the News."[14]

32. NextGen has also failed to provide any explanation for why the notification of consumers about the Data Breach was delayed for nearly a month after the breach was detected. Plaintiffs' and the Class Members' PII could have potentially been in possession of the cybercriminals for almost a month prior to receiving any notification from NextGen. Because NextGen waited so long to disclose the Data Breach and downplayed the risk that patients' PII would be subject to fraud or misuse, NextGen inhibited patients from taking meaningful, proactive, and targeted mitigation measures to protect themselves from harm.

[12] https://www.nextgen.com/ (last accessed May 16, 2023).
[13] https://www.nextgen.com/company/newsroom (last accessed May 16, 2023).
[14] https://www.nextgen.com/company/newsroom/in-the-news (last accessed May 16, 2023).

The Data Breach Was Preventable

33. NextGen's notice to consumers stated that in response to the Data Breach, it "launched an investigation with the help of third-party forensic experts."[15]

34. This reactive action in no way addresses the fact that NextGen should have already had adequate and robust safeguards in place to detect, prevent, and terminate a successful infiltration long before access and exfiltration could reach the PII of over one million patients, as all companies of NextGen's size that store vast amounts of sensitive information should. The only tangible action NextGen disclosed was that it "reset[] passwords." If the Data Breach was so easily contained or remediated, NextGen's failure to prevent the breach is inexcusable given its knowledge that it was an expected target for cyberattacks.

35. NextGen's status as a prime target for cyberattacks was known and obvious to NextGen. This is clear because it disclosed it in its own regulatory filings.[16] NextGen knew that the type of data it collects, maintains, and stores is highly valuable and a frequent target of cybercriminals.

36. In NextGen's 2022 Form 10-K, NextGen acknowledged the known trends:

---

[15] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 16, 2023).

[16] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last accessed May 16, 2023).

> High-profile security breaches at other companies have increased in recent years. And security industry experts and government officials have warned about the risks of hackers and cyber-attacks targeting information technology products and businesses. Although this is an industry-wide problem that affects other software and hardware companies, we may be targeted by computer hackers because we are a prominent healthcare information technology company and have high profile clients. These risks will increase as we continue to . . . store and process increasingly large amounts of our client's confidential data, including personal health information . . . . Moreover, unauthorized access, use or disclosure of such sensitive information, including any resulting from the incidents described above, could result in civil or criminal liability or regulatory action, including potential fines and penalties . . . . These types of security incidents could also lead to lawsuits, regulatory investigations and claims, and increased legal liability.[17]

37. NextGen was aptly aware of its status as a prime target because NextGen had already been a target of such an attack previously this year. In January 2023, NextGen suffered a ransomware attack.[18] In responding to the ransomware attack, NextGen released a statement claiming, "The privacy and security of our client information is of the utmost importance to us."[19]

38. The Federal Trade Commission ("FTC") has issued guidance for addressing the devastating results of data breaches and the harmful effects of an unauthorized person gaining access to someone's PII, warning: "Once identity

---

[17] https://investor.nextgen.com/static-files/c1cd4035-fc46-48ac-8471-8a2170231a3f (last accessed May 16, 2023).
[18] https://www.washingtonpost.com/politics/2023/01/23/latest-cyberattack-health-care-shows-how-vulnerable-sector-is/ (last accessed May 17, 2023).
[19] *Id.*

thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or ger medical treatment on your health insurance."[20]

39. At all times relevant to this Complaint, NextGen was aware of, or reasonably should have known, of the significance and necessity of adequately safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached. Including, specifically, the extensive costs that would be imposed on patients whose PII was accessed as a result of the breach.

40. NextGen knew, or should have known, that because it collected and maintained the PII for a significant number of patients, a significant number of patients would be harmed by a breach of its systems.

41. In spite of the widely available reports regarding cyberattacks, and the fact that NextGen held the PII of millions of patients, NextGen failed to use reasonable care in maintaining the privacy and security of the Plaintiffs and Class Members' PII. If NextGen had implemented common sense security measures and adequate protection, cybercriminals could never have accessed the PII of Plaintiffs and the Class Members, and the Data Breach would have either been prevented in its entirety or much smaller in scope.

[20] https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last accessed May 17, 2023).

NextGen Failed to Comply with Federal Law and Regulations

42. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding such sensitive PII and emphasized the importance of adequate data security practices.[21] The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.[22]

43. The FTC Publication, titled "Protecting Personal Information: A Guide for Business" lays out a fundamental data security principles and standard practices that businesses should be implementing and following to protect PII.[23] The guidelines highlight that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems.[24] The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity,

[21] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed May 17, 2023).
[22] *Id*.
[23] *Id*.
[24] *Id*.

monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.[25]

44. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[26]

45. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

46. NextGen knew or should have known of its obligation to implement and use appropriate measures to protect patients' PII on its systems but failed to comply with the FTC's basic guidelines that would have prevented the Data Breach from occurring or made it much less in scope. NextGen's failure to employ appropriate measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[25] *Id.*
[26] *Id.*

47. NextGen also failed to meet the minimum standards of the National Institute of Standards and Technology ("NIST") Cybersecurity Framework Version 1.1.[27]

Allegations Relating to Plaintiff Christah Ross's Minor Daughter

48. Unbeknownst to Plaintiff Ross, NextGen obtained Plaintiff's minor daughter, K.R.'s PII through one of NextGen's healthcare clients that K.R. had seen as a patient. At the time this Complaint is filed, it is unclear which medical professional provided K.R.'s sensitive PII to NextGen.

49. In May 2023, Plaintiff Ross received a notice letter from NextGen informing her that her twelve-year-old daughter was a victim of the Data Breach. The notice informed Plaintiff Ross that her minor daughter's name, date of birth, address, and Social Security number were all contained in the electronic data accessed in the Data Breach.

50. The letter claimed the cursory information regarding the Data Breach and the remedial steps NextGen was taking and then recommended Plaintiff Ross take certain actions to protect her daughter's identity and credit such as monitoring K.R.'s accounts and "remain[ing] vigilant by reviewing your account statements and

[27] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last accessed May 17, 2023).

credit reports closely."[28] These recommendations read rather ironically as NextGen was not itself vigilant against the risks of the Data Breach to begin with.

51. To prevent additional future harm, Plaintiff Ross' minor daughter has been and will continue to be forced to spend significant time and effort engaging in remedial efforts to protect her information from attacks. Plaintiff Ross must now continue to spend time and effort reviewing her daughter's credit profile and other financial information and accounts for evidence of unauthorized activity. Plaintiff Ross suffered significant distress knowing her daughter's highly sensitive PII is no longer confidential and her son's accounts can be targeted. Given the nature of the information exposed in the Data Breach and the likelihood of cybercriminals to use such sensitive PII to commit a wide array of crimes, K.R. faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and indefinitely.

52. Upon information and belief, NextGen continues to store K.R.'s PII on its internal systems. Thus, K.R. has a continuing interest in ensuring the PII is safeguarded and protected against future breaches.

Allegations Relating to Plaintiff Carter Bundy

[28] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 17, 2023).

53. Unbeknownst to Plaintiff Bundy, NextGen obtained Plaintiff Bundy's minor son, A.B.'s PII through one of NextGen's healthcare clients. At the time this Complaint is filed, it is unclear which medical professional provided A.B.'s PII to NextGen.

54. In May 2023, Plaintiff Bundy received a notice letter from NextGen stating that his twelve-year-old minor son, A.B. was a victim of the Data Breach. The notice informed Plaintiff Bundy that his minor son's name, date of birth, address, and Social Security number were all contained in the electronic data accessed in the Data Breach.

55. The notice recommended that Plaintiff Bundy take certain actions to protect A.B.'s accounts and identity such as monitoring his accounts and "remain[ing] vigilant by reviewing your account statements and credit reports closely."[29] These recommendations read rather ironically as NextGen was not itself vigilant against the risks of the Data Breach to begin with.

56. To protect additional future harm, Plaintiff Bundy has been and will continue to be forced to spend significant time and effort engaging in remedial efforts to protect A.B.'s information from additional attacks. Plaintiff Bundy must now continue to spend time and effort reviewing A.B.'s credit profile and financial

[29] https://dojmt.gov/wp-content/uploads/Consumer-notification-letter-233.pdf (last accessed May 17, 2023).

and other account statements for evidence of unauthorized activity, which he will continue to do indefinitely. Plaintiff Bundy suffered significant distress knowing A.B.'s highly sensitive PII is no longer confidential and his accounts are being targeted. Given the nature of the information exposed in the Data Breach and the likelihood of cybercriminals to use such sensitive information to commit a wide array of financial crimes, A.B. faces a significant present and ongoing risk of identity theft and fraud, financial fraud, and other identity-related fraud now and indefinitely.

57. Upon information and belief, NextGen continues to store A.B.'s PII on its internal systems. Thus, Plaintiff Bundy has a continuing interest in ensuring that the PII is protected and safeguarded from future breaches.

The Impact of the Data Breach on Victims

58. The failure of NextGen to safeguard Plaintiffs' and the Class Members' PII has severe and lasting consequences. Due to the sensitive nature of the PII accessed in the Data Breach—names, dates of birth, and Social Security numbers—cybercriminals can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and indefinitely. As a result, Plaintiffs and the Class Members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

59. The Data Breach exposed PII that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using identity victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities."[30]

60. Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. These identity thieves will also re-use stolen PII, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII.

61. Victims of NextGen's Data Breach face significant harms as the result of the Breach, including, but not limited to, identity theft and financial fraud. Plaintiffs and Class Members are forced to spend time, money, and effort handling the consequences of the Data Breach, including purchasing credit monitoring

[30] "Synthetic identities" refer to instances where an identity thief combines real and fake information to create a new fabricated identity, which is then used to commit fraud.

services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for and responding to unauthorized activity.

62. It is therefore unsurprising that identity theft imposes severe distress on its victims. The 2021 Identity Theft Resource Center survey exemplifies the emotional suffering weathered by victims of identity theft: 84% reported experiencing anxiety, 76% felt violated, 32% experienced financial related identity problems, 83% reported being turned down for credit or loans, 32% reported problems with family members as a result of the breach, and 10% reported feeling suicidal after experiencing the identity theft.[31]

63. Identity theft can cause physical reactions and effects in its victims as well. The same Identity Theft Resource Center survey highlighted that survey respondents experienced physical symptoms after experiencing identity theft, including: 48.3% reported sleep disturbances; 37.1% reported an inability to concentrate or a lack of focus; 28.7% reported they were unable to go to work because of physical symptoms; 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and 12.6% reported a start or relapse into unhealthy or addictive behaviors.[32]

---

[31] https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last accessed May 17, 2023).

[32] https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last accessed May 17, 2023).

64. The unauthorized access to sensitive PII by data thieves also decreases the PII's value to its original owner. Courts have recognized this as its own independent form of harm.[33]

65. Identity theft victims are injured repeatedly each time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. The dark web is made up of several discrete repositories of stolen information that can be aggregated or accessed by different identity thieves with intentions to use each piece of information differently. Each data breach increases the likelihood that a victim's PII will be exposed to more identity thieves who are seeking to misuse it.

66. As a result of the vast array of injuries that can stem from the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harms for which they are entitled to damages, including but not limited to:

a. The unconsented disclosure of confidential information to a third party;

[33] *See* In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig., 440 F. Supp. 3d447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

b. Losing the inherent value of their PII;

c. Losing the value of access to their PII permitted by NextGen;

d. Identity theft and fraud resulting from the theft of their PII;

e. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. Anxiety, emotional distress, and loss of privacy;

g. The present value of ongoing credit monitoring and identity theft protection services necessitated by NextGen's Data Breach;

h. Unauthorized charges and loss of use of and access to their accounts;

i. Lowered credit scores resulting from credit inquiries following fraudulent activities;

j. Costs associated with time spend and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

k. The continued, imminent, and impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or many unauthorized third parties.

67. Even when an individual is reimbursed for a financial loss experienced due to identity theft or fraud, the individual will not be whole again as there is typically significant time and effort expended in seeking and obtaining the reimbursement.

68. There may also be a significant time delay between the theft of the PII and the actual misuse of the stolen information. When conducting a study regarding data breaches, the Government Accountability Office stated: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[34]

69. Reporting on a global consumer survey regarding concerns about privacy and data security, the American Bankers Association noted that 29% of consumers would avoid using a company that had experienced a data breach in the past. The same report notes that 63% of consumers also indicated they would avoid such a company for a period of time.[35]

70. Plaintiffs and Class Members have an interest in NextGen's promises and obligations to safeguard the PII that Plaintiffs and the Class entrusted to their medical care providers. NextGen's failure to live up to its promises and duties in this respect caused Plaintiff and Class Members to seek the present value of ongoing identity protection services to compensate them for the present harm and present and

[34] https://www.gao.gov/assets/gao-07-737.pdf (last accessed May 17, 2023).
[35] https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/ (last accessed May 17, 2023).

continuing increased risk of harm caused by NextGen's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class Members as close to the same position as they would have been in but for NextGen's wrongful conduct, specifically its failure to appropriate and adequately safeguard Plaintiff and Class Members' PII.

71. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their PII permitted through NextGen's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Similar to a technology covered by a trade secret or patent, use or access to an individual's PII is non-rivalrous—the unauthorized use by another does not diminish the original owner's ability to practice the patented invention or use trade-secret protected technology. Nevertheless, Plaintiffs may generally recover the reasonable value of use of the intellectual property, or a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the original owner's own use and even though the owner would not have otherwise licensed such intellectual property to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class Members have protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property

is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

72. NextGen's failure to send prompt notice of the Data Breach also resulted in harm to Plaintiffs and Class Members. The notice Plaintiffs and Class Members received contained no explanation of the precise nature of the Breach, the identity of the cybercriminals, nor the amount of persons affected. NextGen's choice to withhold these essential pieces of information is significant because Class Members may take varying precautions depending on the sensitivity level of information taken and the imminence of the perceived risk. By downplaying the risk of misuse of the PII and delaying notice by nearly a month, NextGen prevented Plaintiffs and Class Members from taking meaningful, proactive, and targeted mitigation measures to secure their PII and accounts.

73. Plaintiffs and Class Members have an interest in ensuring that their PII is adequately safeguarded and not vulnerable to further attacks because NextGen continues to hold their PII.

CLASS ACTION ALLEGATIONS

74. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

All individuals, or if minors, their parents or guardians, NextGen identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.

75. The Class asserts claims against NextGen for negligence (Count I), unjust enrichment (Count II), invasion of privacy (Count III), third-party beneficiary breach of contract (Count IV), bailment (Count V), and breach of fiduciary duty (Count VI).

76. Specifically excluded from the Nationwide Class are NextGen and its officers, directors, or employees; any entity in which NextGen has a controlling interest; and any affiliate, legal representative, heir, or assign of NextGen. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

77. **Jurisdictional Amount.** As alleged herein, Plaintiffs seek damages on behalf of themselves and the over one million putative class members, satisfying the $5 million jurisdictional requirement of 28 U.S.C. § 1332(d)(2).

78. **Ascertainability.** The members of the Class are readily identifiable and ascertainable. NextGen and/or its affiliates, among others, possess the information to identify and contact Class Members.

79. **Numerosity:** The members of the Class are so numerous that joinder of all members' claims is impracticable. NextGen's statements reveal that the Class contains over one million persons whose PII was compromised in the Data Breach.

80. **Typicality:** Plaintiffs' claims are typical of the claims of other members of the Class, in that Plaintiff and the Class Members sustained damages arising out of the same acts and omissions of NextGen relating to its failure to protect, oversee, monitor, and safeguard the PII of Class.

81. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent and protect the interests of other members of the Class. Plaintiffs' claims are made in a representative capacity on behalf of the other members of the Class. Plaintiff has no interests antagonistic to the interests of the other members of the Class and is subject to no unique defenses. Plaintiff has retained competent counsel to prosecute the case on behalf of Plaintiff and the Class. Plaintiff and Plaintiff's counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so.

82. **Policies Generally Applicable to the Class:** This class action is appropriate for certification because NextGen has acted or refused to act on grounds generally applicable to the Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole.

NextGen's practices challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge to those practices hinge on NextGen's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

83. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether NextGen owes Plaintiffs and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

b. Whether NextGen acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class Members' PII;

c. Whether NextGen violated its duty to implement reasonable security systems to protect Plaintiffs' and Class Members' PII

d. Whether NextGen's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class Members;

e. Whether NextGen provided timely notice of the Data Breach to Plaintiffs and Class Members; and

f. Whether Plaintiffs and Class Members are entitled to compensatory damages, punitive damages, and/or nominal damages as a result of the Data Breach.

84. NextGen has engaged in a common course of conduct and Plaintiffs and Class Members have been similarly impacted by NextGen's failure to maintain

adequate security procedures and practices to protect patients' PII, as well as NextGen's failure to timely alert affected patients to the Data Breach.

85. **Superiority:** This case is appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy. Joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small in comparison to the burden and expense of individual prosecutions of litigation necessitated by NextGen's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from NextGen's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties and the court systems of many states and federal districts. By contract, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of sale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

86. Plaintiffs incorporate paragraphs 1-85 as if fully set forth herein.

87. NextGen owed a duty to Plaintiffs and the Class Members to notify them that their PII had been disclosed to and accessed by unauthorized criminal hackers.

88. NextGen owed a duty to Plaintiffs and Class members to properly train, vet, and oversee employees and vendors who maintain, access, store, and manage Plaintiffs' and Class Members' PII and to implement and maintain reasonable data security practices to protect the PII from foreseeable cyberattacks and unauthorized access.

89. NextGen breached these duties and the applicable standards of care by:

a. Failing to conduct proper and reasonable training and due diligence over vendors and employees and data security systems, practices, and procedures;

b. Failing to conduct proper and reasonable due diligence over the employees, vendors, or contractors that were the vector(s) of and/or facilitated the hackers' infiltration into the system(s) storing Plaintiffs' and Class Members' PII;

c. Failing to maintain reasonable and appropriate oversight and audits on its internal data security and its employees, vendors, or contractors that were the vectors of the hackers' infiltration into the system(s) storing Plaintiffs' and Class Members' PII;

d. Failing to adequately segregate and isolate Customer Information from publicly accessible or publicly adjacent environments;

e. Failing to implement and maintain reasonable safeguards and procedures to prevent the unauthorized disclosure of Plaintiffs' and Class Members' PII;

f. Failing to monitor and detect its confidential and sensitive data environment(s) storing Plaintiffs' and Class Members' PII reasonably and appropriately in order to repel or limit the Data Breach;

g. Failing to implement and maintain reasonable data storage and retention procedures with respect to the PII to ensure the PII was being stored and maintained for legitimate and useful purposes;

h. Failing to undertake reasonable and sufficient incident response measures to ensure that the attack directed toward NextGen's sensitive business information would not expose and cause disclosure and unauthorized acquisition of Plaintiffs' and Class Members' PII;

i. Failing to ensure that any and all unauthorized copies of accessed data, including Plaintiffs' and Class Members' PII was deleted,

destroyed, rendered unable to be used, or returned to Plaintiffs and Class Members;

j. Failing to reasonably conduct forensic investigation into the scope, nature, and exposure of the Data Breach or to ascertain its full severity;

k. Failing to provide full disclosure, deceptively misleading consumers through false representations and misleading omissions of fact regarding the Data Breach, consumers' risk and exposure caused by the Data Breach, and the adequacy of the investigation of and response to the Data Breach; and

l. Failing to provide accurate, complete, and sufficiently detailed notification to Plaintiffs and the Class Members regarding the circumstances of the Data Breach, its causes, its effects, the extent of the exposure of the PII, and details regarding the disposition of Plaintiffs' and Class Members' PII at all times during the Data Breach.

90. NextGen is both the actual and legal cause of Plaintiffs' and the Class Members' injuries. Had NextGen adopted and maintained reasonable data security procedures and provided timely notification of the Data breach to those affected, including Plaintiffs and the Class, Plaintiffs and other Class Members would not

have been damaged or would have been damaged to a lesser degree than they actually were.

91. Plaintiffs and Class Members have suffered damages as a result of NextGen's negligence. Plaintiffs and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (d) loss of time and loss of productivity heeding NextGen's warnings and following their instructions on the notices; (e) financial costs incurred due to actual identity theft; (f) the cost of future identity theft monitoring; (g) loss of time incurred due to actual identity theft; and (h) diminution of value of their PII.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

92. Plaintiffs incorporate paragraphs 1-85 as if fully set forth herein.

93. Plaintiffs and Class Members have both an equitable and legal interest in their PII that was conferred upon, collected by, used by, and maintained by NextGen and that was ultimately stolen in the Data Breach.

94. NextGen benefited by the conferral upon it of the PII pertaining to Plaintiffs and the Class Members and by its ability to retain, use, and profit from that information. NextGen understood and valued this benefit.

95. NextGen also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon NextGen maintaining the privacy and confidentiality of such PII.

96. Without NextGen's willingness and commitment to maintain the privacy and confidentiality of the PII, that PII would never have been entrusted to NextGen. If NextGen had disclosed that its data security practices were inadequate, it would not have been permitted to continue in operation by regulators or its clients.

97. Because of NextGen's use of Plaintiffs' and Class Members' PII, NextGen sold more services and products than it otherwise would have. NextGen was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiffs and Class Members.

98. NextGen also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

99. NextGen also benefitted through its unjust conduct in the form of profits it gained through the use of Plaintiffs' and Class Members' PII.

100. It is inequitable for NextGen to retain these benefits.

101. As a result of NextGen's wrongful conduct as alleged in this Complaint—including among other things its failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and Class Members without having adequate data security measures and its other conduct facilitating the theft of the PII—NextGen has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

102. NextGen's unjust enrichment is traceable to and resulted directly and proximately from the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' sensitive PII, while at the same time failing to maintain that information securely and protected from intrusion and theft by hackers and identity thieves.

103. It is inequitable, unfair, and unjust for NextGen to retain these wrongfully obtained benefits. NextGen's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

104. The benefit conferred upon, received, and enjoyed by NextGen was not conferred gratuitously, and it would be inequitable, unfair, and unjust for NextGen to retain the benefit.

105. NextGen's inadequate security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur

substantial time and/or costs mitigating and monitoring the use of their PII and has caused Plaintiffs and Class Members other damages as described herein.

106. Plaintiffs and Class Members have no adequate remedy at law.

107. NextGen is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on NextGen as a result of its wrongful conduct, including specifically: the value to NextGen of the PII that was stolen in the Data Breach; the profits NextGen received and is receiving from the use of that information; and the amounts that NextGen should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

108. Plaintiffs incorporate paragraphs 1-85 as if fully set forth herein.

109. Plaintiffs and Class Members shared PII with NextGen and/or its affiliates that Plaintiffs and Class Members wanted to remain private and non-public.

110. Plaintiffs and Class Members reasonably expected that the PII they shared with NextGen would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

111. NextGen intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a criminal third party.

112. By failing to keep Plaintiffs' and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, NextGen unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, *inter alia*:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their PII properly obtained for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their PII from disclosure to unauthorized persons; and

d. Enabling the disclosures of their PII without consent.

113. The PII that was compromised during the Data Breach was highly sensitive, private, and confidential, as it included Social Security numbers and other information that is the type of sensitive, personal information that one normally expects will be protected from exposure by the entity charged with safeguarding it.

114. NextGen's intrusions into Plaintiffs' and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

115. As a direct and proximate result of NextGen's invasion of privacy, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT IV
THIRD-PARTY BENEFICIARY BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Class)

116. Plaintiffs incorporate paragraphs 1-85 as if fully set forth herein.

117. Acting in the ordinary course of its business, NextGen entered into contracts with medical professionals and healthcare providers to deliver electronic health records software and practice management systems.

118. On information and belief, those respective contracts contained provisions requiring NextGen to protect the PII that NextGen received in order to provide services in turn to the healthcare providers.

119. On information and belief, those provisions requiring NextGen acting in its ordinary course of business to protect PII of the healthcare providers' patients were intentionally included for the direct benefit of Plaintiffs and Class Members, such that Plaintiffs and Class Members are intended third-party beneficiaries of these contracts and are therefore entitled to enforce them.

120. NextGen breached these contracts while acting in the course of its ordinary business by not safeguarding Plaintiffs' and Class Members' PII, as described herein.

121. As a direct and proximate result of NextGen's breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT V
Bailment
(On Behalf of Plaintiffs and the Class)

122. Plaintiffs incorporate paragraphs 1-85 as if fully set forth herein.

123. Plaintiffs and Class Members provided their PII to NextGen—either directly or through business affiliates—which NextGen was under a duty to keep private and confidential.

124. Plaintiffs' minor children and Class Members' PII is personal property, and it was conveyed to NextGen for the certain purpose of keeping the information private and confidential.

125. Plaintiffs' minor children and Class Members' PII has value, and it is highly prized by hackers and cybercriminals. NextGen was aware of the risks it took when accepting their PII for safeguarding, and it assumed the risk voluntarily.

126. Once NextGen accepted Plaintiffs' minor children's and Class Members' PII, it was in the exclusive possession of that PII, and neither Plaintiffs

nor Class Members could control that information once it was within NextGen's possession, custody, and control.

127. NextGen did not safeguard Plaintiffs' or Class Members' PII when it failed to adopt and enforce adequate security safeguards to prevent a known risk of cyberattack.

128. NextGen's failure to safeguard Plaintiffs' and Class Members' PII resulted in their PII being accessed or obtained by third-party cybercriminals.

129. As a result of NextGen's failure to keep Plaintiffs' and Class Members' PII secure, Plaintiffs and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

130. Plaintiffs incorporate paragraphs 1-85 as if fully set forth herein.

131. In light of the special relationship between NextGen and Plaintiffs and Class Members, NextGen became a fiduciary by undertaking a guardianship of the PII to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' minor children's and Class Members' PII; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) NextGen stores.

132. NextGen had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep their PII secure.

133. NextGen breached its fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' PII.

134. NextGen breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PII.

135. As a direct and proximate result of NextGen's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their and their minor children's PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their and their minor children's PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their and their minor children's PII, which remains in NextGen's possession and is vulnerable to further unauthorized disclosures so long as NextGen fails to undertake appropriate and adequate measures to protect the PII

in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, and (vii) the diminished value of NextGen's services they received.

136. As a direct and proximate result of NextGen's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully request the following relief:

A. That the Court certify this action as a class action and appoint Plaintiffs and their Counsel to represent the Class;

B. That the Court grant permanent injunctive relief to prohibit and prevent NextGen from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by NextGen as a result of their unlawful acts, omissions, and practices;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

F. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Respectfully submitted,

Dated: May 22, 2023.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
GA Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 978-6971
Facsimile: (404) 320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Robert C. Schubert (*pro hac vice* to be filed)
Amber L. Schubert (*pro hac vice* to be filed)
SCHUBERT JONCKHEER & KOLBE LLP

2001 Union Street, Suite 200
San Francisco, California 94123
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
rschubert@sjk.law
aschubert@sjk.law

Attorneys for Plaintiffs Ross and Bundy on behalf of their minor children and the Putative Class

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14-point Times New Roman font in accordance with Local Rule 5.1(C).

Dated: May 22, 2023.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON